Results on Vertex Degree and K-Connectivity in Uniform S-Intersection Graphs

Jun Zhao, Osman Yagan and Virgil Gligor

January 1, 2014

CMU-CyLab-14-004

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **01 JAN 2014**	2. REPORT TYPE	3. DATES COVERED **00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE **Results on vertex degree and k-connectivity in uniform s-intersection graphs**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,CyLab,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

We present results related to the vertex degree in a uniform s-intersection graph which has received much interest recently. Specif- ically, we derive the probability distribution for the minimum vertex degree, and show that the number of vertices with an arbitrary degree converges to a Poisson distribution. A uniform s-intersection graph mod- els the topology of a secure wireless sensor network employing the widely used s-composite key predistribution scheme. Our theoretical findings is also confirmed by numerical results.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**14**	

Results on vertex degree and *k*-connectivity in uniform s-intersection graphs

Jun Zhao, Osman Yağan and Virgil Gligor

CyLab and Dept. of ECE
Carnegie Mellon University
{junzhao,oyagan,virgil}@andrew.cmu.edu

Abstract. We present results related to the vertex degree in a uniform s-intersection graph which has received much interest recently. Specifically, we derive the probability distribution for the minimum vertex degree, and show that the number of vertices with an arbitrary degree converges to a Poisson distribution. A uniform s-intersection graph models the topology of a secure wireless sensor network employing the widely used s-composite key predistribution scheme. Our theoretical findings is also confirmed by numerical results.

Keywords: Key predistribution, random intersection graphs, wireless sensor networks, vertex degree.

1 Introduction

The uniform s-intersection graphs have received much attention recently [1–3, 8, 11, 12]. Such graphs are induced by the s-composite key predistribution scheme [5], which has been recognized as a typical solution to secure communication in wireless sensor networks [3, 7, 9–12].

The uniform s-intersection graph is defined as follows. For a graph with n vertices, each vertex independently selects X_n different items uniformly at random from a pool comprising Y_n items. X_n and Y_n are both functions of n, with the natural condition $1 \leq X_n \leq Y_n$. There exists an edge between two different vertices if and only if they have at least s items in common, where $1 \leq s \leq X_n$. For a secure wireless sensor network employing the s-composite key predistribution scheme [5], when the network is modeled by a uniform s-intersection graph, vertices in the graph correspond to nodes in the network; and the items on each vertex corresponds to the cryptographic keys on each sensor.

In this paper, we report results on the vertex degree in uniform s-intersection graphs. The degree of a vertex v is the number of vertices having edges with v; and the minimum (vertex) degree of a graph is the least among the degrees of all vertices. Specifically, we obtain the asymptotic probability distribution for the minimum degree, and demonstrate that the number of vertices with an arbitrary degree asymptotically converges to a Poisson distribution.

The rest of the paper is organized as follows. We discuss the graph notation in Section 2. Section 3 presents the results. Section 6 offers numerical experiments to confirm our analytical results. In Section 7, we report relevant results in the literature. Section 8 concludes the paper.

2 Notation

We use $G_s(n, X_n, Y_n)$ to denote a uniform s-intersection graph defined in Section 1. Throughout the paper, s is a positive integer and does not scale with n. Let the vertex set of $G_s(n, X_n, Y_n)$ be $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$. For each vertex $v_i \in \mathcal{V}$, the set of its X_n different items is denoted by S_i. Two distinct vertices v_i and v_j $(1 \leq i < j \leq n)$ establish an edge in between if and only if $\big[|S_i \cap S_j| \geq s\big]$, where $|A|$ for set A signifies the cardinality of A. Let p_u be the edge probability. With $\mathbb{P}[\mathcal{E}]$ denoting the probability of event $\mathcal{E}$ throughout the paper, we obtain

$$p_u = \mathbb{P}[|S_i \cap S_j| \geq s].$$

3 The Results

We detail the results for graph $G_s(n, X_n, Y_n)$ in Theorems 1 and 2 below. We use the standard asymptotic notation $o(\cdot), O(\cdot), \Theta(\cdot), \sim$. In particular, for two positive functions $f(n)$ and $g(n)$, we write $f(n) \sim g(n)$ if and only if $\lim_{n\to\infty} [f(n)/g(n)] = 1$.

Theorem 1 *For graph $G_s(n, X_n, Y_n)$ with*

$$X_n = \omega(1), \tag{1}$$

for some positive integer h and some sequence γ_n satisfying

$$-1 < \liminf_{n\to\infty} \frac{\gamma_n}{\ln\ln n} \leq \limsup_{n\to\infty} \frac{\gamma_n}{\ln\ln n} < 1, \tag{2}$$

and having $\lim_{n\to\infty} \gamma_n$ $(\lim_{n\to\infty} \gamma_n \in [-\infty, \infty])$, consider

$$\frac{\left[X_n(X_n-1)\ldots(X_n-(s-1))\right]^2}{s!{Y_n}^s} = \frac{\ln n + (h-1)\ln\ln n + \gamma_n - \ln[(h-1)!]}{n}. \tag{3}$$

Then properties (a) and (b) below hold.

(a) With d denoting the minimum vertex degree of $G_s(n, X_n, Y_n)$, we have

$$\lim_{n\to\infty} \mathbb{P}[d = h] = \exp\Big\{ -\exp\big\{ -\lim_{n\to\infty} \gamma_n \big\}\Big\},$$
$$\lim_{n\to\infty} \mathbb{P}[d = h-1] = 1 - \exp\Big\{ -\exp\big\{ -\lim_{n\to\infty} \gamma_n \big\}\Big\},$$

and

$$\lim_{n\to\infty} \mathbb{P}[(d < h-1) \text{ or } (d > h)] = 0.$$

(b) The number of nodes with degree r converges to a Poisson distribution, and its mean λ_r satisfies

$$\lim_{n\to\infty} \lambda_r = \begin{cases} 0, & \text{for } r = 0, 1, \dots, h-2, \\ \exp\big\{-\lim_{n\to\infty} \gamma_n\big\}, & \text{for } r = h-1, \\ \infty, & \text{for } r = h, h+1, \dots. \end{cases}$$

Theorem 1 for graph $G_s(n, X_n, Y_n)$ presents the asymptotic probability distribution for the minimum vertex degree, and the asymptotic Poisson distribution for the number of nodes with an arbitrary degree.

Remark 1 *From property (a) of Theorem 1 above, it is clear that*

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\text{Graph } G_s(n, X_n, Y_n) \text{ has a} \\ \text{minimum vertex degree at least } h.\end{array}\right] = \exp\Big\{-\exp\big\{-\lim_{n\to\infty}\gamma_n\big\}\Big\}.$$

Remark 2 *Note that $e^{\infty} = \infty$ and $e^{-\infty} = 0$. Therefore,*

- *if* $\lim_{n\to\infty} \gamma_n = \infty$, *then* $\exp\big\{-\lim_{n\to\infty} \gamma_n\big\} = 0$ *and* $\exp\Big\{-\exp\big\{-\lim_{n\to\infty}\gamma_n\big\}\Big\} = 1$*; and*
- *if* $\lim_{n\to\infty} \gamma_n = -\infty$, *then* $\exp\big\{-\lim_{n\to\infty} \gamma_n\big\} = \infty$ *and* $\exp\Big\{-\exp\big\{-\lim_{n\to\infty}\gamma_n\big\}\Big\} = 0$.

We give Theorem 2 below as an analog of Theorem 1, with the complex expression in L.H.S. (left hand side) of (3) replaced by $\frac{1}{s!}\big(\frac{{X_n}^2}{Y_n}\big)^s$, under the cost of a more constrained condition on X_n compared to (1).

Theorem 2 *For graph $G_s(n, X_n, Y_n)$ with*

$$X_n = \omega(\ln n), \tag{4}$$

for some positive integer h and some sequence γ_n satisfying (2) and having $\lim_{n\to\infty} \gamma_n$ ($\lim_{n\to\infty} \gamma_n \in [-\infty, \infty]$), consider

$$\frac{1}{s!}\left(\frac{{X_n}^2}{Y_n}\right)^s = \frac{\ln n + (h-1)\ln\ln n + \gamma_n - \ln[(h-1)!]}{n}, \tag{5}$$

Then properties (a) and (b) of Theorem 1 hold.

Remark 3 *Under the conditions of Theorem 1 or 2, below we show that it always holds that*

$$\frac{{X_n}^2}{Y_n} = O\left(\left(\frac{\ln n}{n}\right)^{\frac{1}{s}}\right). \tag{6}$$

Under the conditions of Theorem 1, from (1) and (3), we have

$$\begin{aligned} \frac{1}{s!}\left(\frac{{X_n}^2}{Y_n}\right)^s &= \frac{\left[X_n(X_n-1)\dots(X_n-(s-1))\right]^2}{s!{Y_n}^s} \cdot [1+o(1)] \\ &= \left[\frac{\ln n + (h-1)\ln\ln n + \gamma_n - \ln[(h-1)!]}{n}\right] \cdot [1+o(1)]. \end{aligned} \tag{7}$$

From $\limsup_{n\to\infty} \frac{\gamma_n}{\ln\ln n} < 1$ *given (2), we obtain* $\frac{\gamma_n}{\ln\ln n} < 1$ *for all* n *sufficient large. Therefore, it holds that for all* n *sufficient large,*

$$\frac{\ln n + (h-1)\ln\ln n + \gamma_n - \ln[(h-1)!]}{n} < \frac{\ln n + h\ln\ln n}{n}. \tag{8}$$

Under the conditions of Theorem 1 or 2, we have either (7) or (5). In view of (8), we further obtain

$$\frac{1}{s!}\left(\frac{{X_n}^2}{Y_n}\right)^s \leq \frac{\ln n + h\ln\ln n}{n} \cdot [1+o(1)] = O\left(\frac{\ln n}{n}\right),$$

which clearly leads to (6).

4 Evaluating the Edge Probability p_u

We present Lemma 1 to evaluate the edge probability p_u.

Lemma 1 *The properties (a) and (b) below hold.*

(a) If $\lim_{n\to\infty} \frac{{X_n}^2}{Y_n} = 0$ *and* $X_n \geq s$ *for all* n *sufficiently large, then*

$$p_u = \frac{[X_n(X_n-1)\dots(X_n-(s-1))]^2}{s!{Y_n}^s} \cdot \left[1 \pm O\left(\frac{{X_n}^2}{Y_n}\right)\right]. \tag{9}$$

(b) If $\lim_{n\to\infty} \frac{{X_n}^2}{Y_n} = 0$ *and* $\lim_{n\to\infty} X_n = \infty$*, then*

$$p_u = \frac{1}{s!}\left(\frac{{X_n}^2}{Y_n}\right)^s \cdot \left[1 \pm O\left(\frac{{X_n}^2}{Y_n}\right) \pm O\left(\frac{1}{X_n}\right)\right]. \tag{10}$$

Before proving Lemma 1 in Section 4.1, we explain the following result given Lemma 1: under the conditions of Theorem 1 or 2, there always exists some sequence $\gamma_n^* = \gamma_n \pm o(1)$ such that

$$p_u = \frac{\ln n + (h-1)\ln\ln n + \gamma_n^* - \ln[(h-1)!]}{n}. \tag{11}$$

We now demonstrate (11) using the following Lemma 2, the proof of which is deferred to Section 4.2.

Lemma 2 *For some* h *and some sequence* γ_n *satisfying (2), we have*

$$\frac{\ln n + (h-1)\ln\ln n + \gamma_n - \ln[(h-1)!]}{n} \sim \frac{\ln n}{n}.$$

(i) We first consider the case where the conditions of Theorem 1 hold. From Remark 3, we have (6), leading to $\lim_{n\to\infty} \frac{{X_n}^2}{Y_n} = 0$. From (1), it follows that $X_n \geq s$

for all n sufficiently large. Then we use property (a) of Lemma 1 to obtain (9). For γ_n satisfying (2), from (3) and Lemma 2,

$$\frac{[X_n(X_n-1)\dots(X_n-(s-1))]^2}{s!{Y_n}^s} \sim \frac{\ln n}{n}. \tag{12}$$

Substituting (3) and (12) to (9), we obtain

$$\begin{aligned} p_u &= \frac{\ln n+(h-1)\ln\ln n+\gamma_n}{n} \pm O\bigg(\frac{\ln n}{n}\bigg)\cdot O\bigg(\bigg(\frac{\ln n}{n}\bigg)^{\frac{1}{s}}\bigg). \\ &= \frac{\ln n+(h-1)\ln\ln n+\gamma_n \pm o(1)}{n}. \end{aligned} \tag{13}$$

(ii) We now consider the case where the conditions of Theorem 2 hold. From Remark 3, we have (6), leading to $\lim_{n\to\infty}\frac{{X_n}^2}{Y_n}=0$. From (4), it follows that $\lim_{n\to\infty} X_n=\infty$. Then we use property (b) of Lemma 1 to obtain (10). Substituting (4) (5) and (6) to (10), we obtain

$$\begin{aligned} p_u &= \frac{\ln n+(h-1)\ln\ln n+\gamma_n}{n} \pm O\bigg(\frac{\ln n}{n}\bigg)\cdot \bigg[\pm O\bigg(\bigg(\frac{\ln n}{n}\bigg)^{\frac{1}{s}}\bigg) \pm o\bigg(\frac{1}{\ln n}\bigg)\bigg]. \\ &= \frac{\ln n+(h-1)\ln\ln n+\gamma_n \pm o(1)}{n}. \end{aligned} \tag{14}$$

Summarizing cases (i) and (ii) above, with γ_n^* defined by (11), we obtain from (13) and (14) that $\gamma_n^*=\gamma_n\pm o(1)$.

4.1 The Proof of Lemma 1

We demonstrate properties (a) and (b) of Lemma 1 below.

Establishing Property (a):

By definition, the edge probability is expressed by

$$p_u=\sum_{r=s}^{X_n}\mathbb{P}[|S_i\cap S_j|=r].$$

From $\lim_{n\to\infty}\frac{{X_n}^2}{Y_n}=0$, it holds that $Y_n\geq 2X_n$ for all n sufficiently large. Then as given in our work [13], we have

$$\mathbb{P}[|S_i\cap S_j|=r]=\frac{\binom{X_n}{r}\binom{Y_n-X_n}{X_n-r}}{\binom{Y_n}{X_n}}. \tag{15}$$

We will demonstrate the following (16) and (17).

$$\mathbb{P}[|S_i\cap S_j|=s]=\frac{[X_n(X_n-1)\dots(X_n-(s-1))]^2}{s!{Y_n}^s}\cdot\bigg[1\pm O\bigg(\frac{{X_n}^2}{Y_n}\bigg)\bigg], \tag{16}$$

and

$$\frac{\sum_{r=s+1}^{X_n} \mathbb{P}[|S_i \cap S_j| = r]}{\mathbb{P}[|S_i \cap S_j| = s]} = O\left(\frac{{X_n}^2}{Y_n}\right). \tag{17}$$

Once (16) and (17) is proved, with $\lim_{n\to\infty} \frac{{X_n}^2}{Y_n} = 0$, we have

$$\begin{aligned}
p_u &= \sum_{r=s}^{X_n} \mathbb{P}[|S_i \cap S_j| = r] \\
&= \mathbb{P}[|S_i \bigcap S_j| = s] \cdot \left\{1 + \frac{\sum_{r=s+1}^{X_n} \mathbb{P}[|S_i \cap S_j| = r]}{\mathbb{P}[|S_i \cap S_j| = s]}\right\} \\
&= \frac{[X_n(X_n-1)\dots(X_n-(s-1))]^2}{s!{Y_n}^s} \cdot \left[1 \pm O\left(\frac{{X_n}^2}{Y_n}\right)\right] \cdot \left[1 + O\left(\frac{{X_n}^2}{Y_n}\right)\right] \\
&= \frac{[X_n(X_n-1)\dots(X_n-(s-1))]^2}{s!{Y_n}^s} \cdot \left[1 \pm O\left(\frac{{X_n}^2}{Y_n}\right)\right];
\end{aligned}$$

i.e., the property (a) of Lemma 1 holds.

We start with showing (16). From (15), it follows that

$$\begin{aligned}
\mathbb{P}[|S_i \bigcap S_j| = s] &= \frac{\binom{X_n}{s}\binom{Y_n - X_n}{X_n - s}}{\binom{Y_n}{X_n}} \\
&= \frac{1}{s!}\left[\frac{X_n!}{(X_n-s)!}\right]^2 \cdot \frac{(Y_n - X_n)!}{(Y_n - 2X_n + s)!} \cdot \frac{(Y_n - X_n)!}{Y_n!}. \qquad (18)
\end{aligned}$$

Then

$$\begin{aligned}
&\mathbb{P}[|S_i \bigcap S_j| = s] \Big/ \left\{\frac{[X_n(X_n-1)\dots(X_n-(s-1))]^2}{s!{Y_n}^s}\right\} \qquad (19) \\
&= {Y_n}^s \cdot \frac{(Y_n - X_n)!}{(Y_n - 2X_n + s)!} \cdot \frac{(Y_n - X_n)!}{Y_n!} \\
&= {Y_n}^s \cdot \left[\prod_{\ell=0}^{X_n - s - 1} (Y_n - X_n - \ell)\right] \cdot \prod_{\ell=0}^{X_n - 1} \frac{1}{Y_n - \ell} \\
&= \prod_{\ell=0}^{X_n - 1} \frac{Y_n}{Y_n - \ell} \prod_{\ell=0}^{X_n - s - 1} \frac{Y_n - X_n - \ell}{Y_n} \\
&= \left[\prod_{\ell=0}^{X_n - s - 1} \left(1 - \frac{X_n + \ell}{Y_n}\right)\right] \Big/ \left[\prod_{\ell=0}^{X_n - 1} \left(1 - \frac{\ell}{Y_n}\right)\right]. \qquad (20)
\end{aligned}$$

By [11, Fact 2(b)], we have

$$\prod_{\ell=0}^{X_n - s - 1} \left(1 - \frac{X_n + \ell}{Y_n}\right) \geq \left(1 - \frac{2X_n}{Y_n}\right)^{X_n} \geq 1 - \frac{2{X_n}^2}{Y_n} \tag{21}$$

and

$$\prod_{\ell=0}^{X_n-1}\left(1-\frac{\ell}{Y_n}\right) \geq \left(1-\frac{X_n}{Y_n}\right)^{X_n} \geq 1-\frac{{X_n}^2}{Y_n}. \tag{22}$$

In addition,

$$\prod_{\ell=0}^{X_n-s-1}\left(1-\frac{X_n+\ell}{Y_n}\right) \leq 1 \tag{23}$$

and

$$\prod_{\ell=0}^{X_n-1}\left(1-\frac{\ell}{Y_n}\right)\left(1-\frac{X_n}{Y_n}\right)^{X_n} \leq 1. \tag{24}$$

Applying (21) and (24) to (20), we obtain

$$(19) \geq 1-\frac{2{X_n}^2}{Y_n}. \tag{25}$$

From $\lim\limits_{n\to\infty}\frac{{X_n}^2}{Y_n}=0$, it holds that for all n sufficiently large

$$\left(1+\frac{2{X_n}^2}{Y_n}\right)\left(1-\frac{{X_n}^2}{Y_n}\right) = 1+\frac{{X_n}^2}{Y_n}-2\left(\frac{{X_n}^2}{Y_n}\right)^2 \geq 1.$$

Then applying (22) and (23) to (20), we obtain

$$(19) \leq \frac{1}{1-\frac{{X_n}^2}{Y_n}} \leq 1+\frac{2{X_n}^2}{Y_n}. \tag{26}$$

Clearly, (16) is proved in view of (25) and (26).

We now demonstrate (17). From (15),

$$\begin{aligned}
&\frac{\sum_{r=s+1}^{X_n}\mathbb{P}[|S_{ij}|=r]}{\mathbb{P}[|S_{ij}|=s]}\\
&=\sum_{r=s+1}^{X_n}\left[\binom{X_n}{r}\binom{Y_n-X_n}{X_n-r}\Big/\binom{X_n}{s}\binom{Y_n-X_n}{X_n-s}\right]\\
&=\sum_{r=s+1}^{X_n}\left\{\frac{s!}{r!}\left[\frac{(X_n-s)!}{(X_n-r)!}\right]^2\frac{(Y_n-2X_n+s)!}{(Y_n-2X_n+r)!}\right\} \quad \left(\text{by } \binom{r}{s}\geq 1 \text{ for } r>s\right)\\
&\leq\sum_{r=s+1}^{X_n}\left[\frac{1}{(r-s)!}\cdot{X_n}^{2(r-s)}\cdot(Y_n-2X_n)^{s-r}\right]\\
&\leq e^{\frac{{X_n}^2}{Y_n-2X_n}}-1 \quad (\text{by Taylor series})\\
&=O\left(\frac{{X_n}^2}{Y_n}\right).
\end{aligned}$$

Property (a) of Lemma 1 is proved with (16) and (17).

Establishing Property (b):

From condition $\lim_{n\to\infty} X_n = \infty$, we have $X_n > s$ for all n sufficiently large, leading to

$$X_n(X_n-1)\dots(X_n-(s-1)) \geq (X_n-s)^s = {X_n}^s \cdot \left(1-\frac{s}{X_n}\right)^s.$$

By [11, Fact 2(b)], we further obtain

$$X_n(X_n-1)\dots(X_n-(s-1)) \geq {X_n}^s \cdot \left(1-\frac{s^2}{X_n}\right),$$

which together with $X_n(X_n-1)\dots(X_n-(s-1)) \leq {X_n}^s$ yields

$$X_n(X_n-1)\dots(X_n-(s-1)) = {X_n}^s \cdot \left[1-O\left(\frac{1}{X_n}\right)\right]. \tag{27}$$

Given $\lim_{n\to\infty} \frac{{X_n}^2}{Y_n} = 0$ and $X_n > s$ for all n sufficiently large, we use property (a) of Lemma 1 to obtain (9). Substituting (27) into (9), we get

$$p_u = {X_n}^s \cdot \left[1-O\left(\frac{1}{X_n}\right)\right] \cdot \left[1 \pm O\left(\frac{{X_n}^2}{Y_n}\right)\right],$$

which along with $\frac{{X_n}^2}{Y_n} = o(1)$ leads to (10).

4.2 The Proof of Lemma 2

Given (2), then for all n sufficient large, we obtain $-1 < \frac{\gamma_n}{\ln\ln n} < 1$, leading to

$$-\ln\ln n < \gamma_n < \ln\ln n. \tag{28}$$

From (28), it is clear that

$$\frac{\ln n + (h-1)\ln\ln n + \gamma_n - \ln[(h-1)!]}{n} \sim \frac{\ln n}{n}.$$

5 Establishing Theorems 1 and 2

As shown in Section 4, under the conditions of Theorem 1 or 2, we have

$$p_u = \frac{\ln n + (h-1)\ln\ln n + \gamma_n^* - \ln[(h-1)!]}{n}, \tag{29}$$

where γ_n satisfies (2) and γ_n^* satisfies

$$\gamma_n^* = \gamma_n \pm o(1). \tag{30}$$

Based on (29), we further derive $p_u \sim \frac{\ln n}{n}$ below. From (2) and (30), we obtain

$$-1 < \liminf_{n\to\infty} \frac{\gamma_n^*}{\ln\ln n} \leq \limsup_{n\to\infty} \frac{\gamma_n^*}{\ln\ln n} < 1; \tag{31}$$

i.e., (2) with γ_n replaced by γ_n^* holds. Then from (29) (31) and Lemma 2, it follows that

$$p_u \sim \frac{\ln n}{n}. \tag{32}$$

We denote by $G(n, p_n)$ an Erdős–Rényi graph [6] defined on a set of n nodes such that two vertices have an edge in between with probability p_n, independent of other vertices. We have proved in our technical report [13] that with M_r denoting the number of vertices with degree r in graph $G_s(n, X_n, Y_n) \cap G(n, p_n)$, where $r = 0, 1, \ldots$, if $\lim\limits_{n\to\infty} X_n = \infty$, $\lim\limits_{n\to\infty} \frac{{X_n}^2}{Y_n} = 0$ and $p_u p_n \sim \frac{\ln n}{n}$, then M_r converges to a Poisson distribution with mean

$$\chi_r := n(r!)^{-1}(np_u p_n)^r e^{-np_u p_n}.$$

Under the conditions of Theorem 1 or 2, we always have $\lim\limits_{n\to\infty} X_n = \infty$ (from either (1) or (5)), $\lim\limits_{n\to\infty} \frac{{X_n}^2}{Y_n} = 0$ (from Remark 3) and $p_u \sim \frac{\ln n}{n}$ (proved above). Note that graph $G_s(n, X_n, Y_n) \cap G(n, p_n)$ with $p_n = 1$ is exactly graph $G_s(n, X_n, Y_n)$. Hence, with L_r denoting the number of vertices with degree r in graph $G_s(n, X_n, Y_n)$, where $r = 0, 1, \ldots$, then under the conditions of Theorem 1 or 2, L_r converges to a Poisson distribution with mean

$$\lambda_r := n(r!)^{-1}(np_u)^r e^{-np_u}. \tag{33}$$

Applying (29) and (32) to (34), we have

$$\begin{aligned}
\lambda_r &\sim n(r!)^{-1}(\ln n)^r e^{-\ln n - (h-1)\ln\ln n - \gamma_n^* + \ln[(h-1)!]} \\
&= n(r!)^{-1}(\ln n)^r \cdot n^{-1}(\ln n)^{-(h-1)} e^{-\gamma_n^*} \cdot (h-1)! \\
&= (r!)^{-1}(h-1)! e^{-\gamma_n^*}(\ln n)^{r+1-h}.
\end{aligned} \tag{34}$$

For $r = h - 1$, from (34), it holds that

$$\lambda_r = \lambda_{h-1} \sim e^{-\gamma_n^*}. \tag{35}$$

Under the conditions of Theorem 1 or 2, $\lim\limits_{n\to\infty} \gamma_n$ exists and we have $\lim\limits_{n\to\infty} \gamma_n \in [-\infty, \infty]$. From (30), it follows that $\lim\limits_{n\to\infty} \gamma_n = \lim\limits_{n\to\infty} \gamma_n^*$. Then using (35), we obtain the following three cases.

- If $\lim\limits_{n\to\infty} \gamma_n = x$, then $\lim\limits_{n\to\infty} e^{-\gamma_n} = e^{-x}$ and $\lim\limits_{n\to\infty} \lambda_{h-1} = e^{-x}$.
- If $\lim\limits_{n\to\infty} \gamma_n = \infty$, then $\lim\limits_{n\to\infty} e^{-\gamma_n} = 0$ and $\lim\limits_{n\to\infty} \lambda_{h-1} = 0$.

- If $\lim_{n\to\infty} \gamma_n = -\infty$, then $\lim_{n\to\infty} e^{-\gamma_n} = \infty$ and $\lim_{n\to\infty} \lambda_{h-1} = \infty$.

Summarizing the three cases above, it is clear that

$$\lim_{n\to\infty} \lambda_{h-1} = \exp\big\{-\lim_{n\to\infty}\gamma_n\big\}. \tag{36}$$

Given (31), we select two constants c_1 and c_2 such that

$$-1 < c_1 < \liminf_{n\to\infty} \frac{\gamma_n^*}{\ln\ln n} \leq \limsup_{n\to\infty} \frac{\gamma_n^*}{\ln\ln n} < c_2 < 1. \tag{37}$$

Then for all n sufficient large, we have $-1 < c_1 < \frac{\gamma_n^*}{\ln\ln n} < c_2 < 1$, resulting in

$$c_1 \ln\ln n < \gamma_n^* < c_2 \ln\ln n. \tag{38}$$

For $r \geq h$, using (38) in (34), we obtain

$$\begin{aligned}\lambda_r &\geq (r!)^{-1}(h-1)! e^{-\gamma_n^*} \ln n \cdot [1-o(1)]\\ &\geq (r!)^{-1}(h-1)! e^{-c_2 \ln\ln n - o(1)} \ln n \cdot [1-o(1)]\\ &= \Omega\big((\ln n)^{1-c_2}\big)\\ &\to \infty, \text{ as } n\to\infty,\end{aligned} \tag{39}$$

in view of $c_2 < 1$ from (37).

For $r \leq h-2$, using (38) in (34), we obtain

$$\begin{aligned}\lambda_r &\leq (r!)^{-1}(h-1)! e^{-\gamma_n^*} (\ln n)^{-1} \cdot [1+o(1)]\\ &\geq (r!)^{-1}(h-1)! e^{-c_1 \ln\ln n + o(1)} (\ln n)^{-1} \cdot [1+o(1)]\\ &= O\big((\ln n)^{-1-c_1}\big)\\ &\to 0, \text{ as } n\to\infty,\end{aligned} \tag{40}$$

in view of $c_1 > -1$ from (37).

Summarizing (36) (39) and (40), we obtain

$$\lim_{n\to\infty} \lambda_r = \begin{cases} 0, & \text{for } r = 0,1,\ldots,h-2,\\ \exp\big\{-\lim_{n\to\infty}\gamma_n\big\}, & \text{for } r = h-1,\\ \infty, & \text{for } r = h, h+1, \ldots. \end{cases} \tag{41}$$

Then for each of Theorems 1 and 2, its property (b) holds.

Given λ_h in (41), the process of evaluating $\mathbb{P}[d=h]$ is similar to the technique in [13, Section IV]. Due to the space limitation, we do not repeat the details. Finally, for each of Theorems 1 and 2, its property (a) follows.

6 Numerical Experiments

We present numerical experiments below to support the theoretical results. For graph $G_s(n, X, Y)$, where n is the number of vertices, X is the number of items

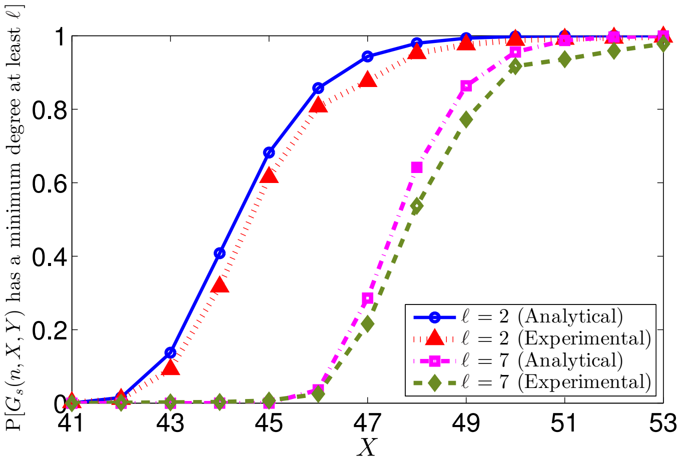

Fig. 1. A plot of the probability that the minimum vertex degree of graph $G_s(n,X,Y)$ is no less than ℓ for $\ell = 2$ or $\ell = 7$ with $n = 1,000$, $Y = 20,000$ and $s = 2$.

for each vertex, and Y is the item pool size, we set $n = 1,000$, $Y = 20,000$ and $s = 2$. Figure 1 depicts both the analytical and experimental curves for the probability that graph $G_s(n,X,Y)$ has a minimum vertex degree at least ℓ with $\ell = 2$ or $\ell = 7$. For the analytical curves, we use the results in Theorem 1; namely, we first compute γ satisfying

$$\frac{[X(X-1)\dots(X-(s-1))]^2}{s!Y^s} = \frac{\ln n + (\ell-1)\ln\ln n + \gamma - \ln[(\ell-1)!]}{n}.$$

Then we use $e^{-e^{-\gamma}}$ as the analytical value for the probability that graph $G_s(n,X,Y)$ has a minimum vertex degree at least ℓ. For the experimental curves, we generate $1,000$ samples of $G_s(n,X,Y)$ and count the times where the minimum vertex degree is no less than ℓ. We divide the counts by $1,000$ to derive the empirical probabilities. As illustrated in Figure 1, the simulation results confirm our theoretical findings.

7 Related Work

For graph $G_s(n,X_n,Y_n)$, Bloznelis and Łuczak [4] recently consider the following three properties: (i) the graph has a minimum vertex degree at least 1; (ii) the graph has a perfect matching; (iii) the graph is connected. They present that when n is even, for each of these three properties, its probability converges to $\exp\left\{-\exp\left\{-\lim_{n\to\infty}\alpha_n\right\}\right\}$ as $n \to \infty$, under conditions $p_u = \frac{\ln n + \alpha_n}{n}$ (p_u is the edge probability), $p_u = O\left(\frac{\ln n}{n}\right)$ and $\left\{(s+2)\left[\binom{K_n}{s}\right]^5(\ln\ln n)^2\right\}^{\frac{3K_n-s}{3(K_n-s)}} \leq (\ln n)^\beta$ for some $\beta \in (0,1)$.

Bloznelis [1] investigates the clustering coefficient of graph $G_s(n, X_n, Y_n)$ and show that the chance of two neighbors of a given vertex v to be adjacent decays as cd^{-1}, where c is a positive constant and d is the degree of vertex v. Bloznelis *et al.* [2] study the correlation coefficient of degrees of adjacent vertices in $G_s(n, X_n, Y_n)$. Bloznelis *et al.* [3] demonstrate that a connected component in $G_s(n, X_n, Y_n)$ with at at least a constant fraction of n emerges as $n \to \infty$ when the edge probability $p_{u,s}$ exceeds $1/n$.

8 Conclusion

In this paper, we derive results for several topological properties related to the vertex degree in a uniform s-intersection graph. We also present numerical experiments to confirm our analytical results.

Acknowledgements

This research was supported in part by CyLab at Carnegie Mellon University under grant DAAD19-02-1-0389 from the US Army Research Office. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of any sponsoring institution, the U.S. government or any other entity.

References

1. M. Bloznelis. Degree and clustering coefficient in sparse random intersection graphs. *The Annals of Applied Probability*, 23(3):1254–1289, 2013.
2. M. Bloznelis, J. Jaworski, and V. Kurauskas. Assortativity and clustering of sparse random intersection graphs. *Electron. J. Probab.*, 18:no. 38, 1–24, 2013.
3. M. Bloznelis, J. Jaworski, and K. Rybarczyk. Component evolution in a secure wireless sensor network. *Netw.*, 53:19–26, January 2009.
4. M. Bloznelis and T. Łuczak. Perfect matchings in random intersection graphs. *Acta Mathematica Hungarica*, 138(1-2):15–33, 2013.
5. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proc. of IEEE Symposium on Security and Privacy*, May 2003.
6. P. Erdős and A. Rényi. On random graphs, I. *Publicationes Mathematicae (Debrecen)*, 6:290–297, 1959.
7. K. Krzywdziński and K. Rybarczyk. Geometric graphs with randomly deleted edges – connectivity and routing protocols. *Mathematical Foundations of Computer Science*, 6907:544–555, 2011.
8. O. Yağan. *Random Graph Modeling of Key Distribution Schemes in Wireless Sensor Networks*. PhD thesis, Dept. of ECE, College Park (MD), June 2011. Available online at `http://hdl.handle.net/1903/11910`.
9. O. Yağan. Performance of the Eschenauer-Gligor key distribution scheme under an on/off channel. *IEEE Transactions on Information Theory*, 58(6):3821–3835, June 2012.
10. O. Yağan and A. M. Makowski. Zero-one laws for connectivity in random key graphs. *IEEE Transactions on Information Theory*, 58(5):2983–2999, May 2012.

11. J. Zhao, O. Yağan, and V. Gligor. k-Connectivity in secure wireless sensor networks with physical link constraints — the on/off channel model. *Arxiv*, 2012. Available online at `http://arxiv.org/abs/1206.1531v1`.
12. J. Zhao, O. Yağan, and V. Gligor. Secure k-connectivity in wireless sensor networks under an on/off channel model. In *Proc. of IEEE ISIT*, pages 2790–2794, 2013.
13. J. Zhao, O. Yağan, and V. Gligor. Topological properties of wireless sensor networks under the q-composite key predistribution scheme with unreliable links. Technical Report CMU-CyLab-14-002, CyLab, Carnegie Mellon University, 2014. Available online at
`http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab14002.pdf` .